ViRobot
Windows Server 3.5

User's Guide

ViRobot Windows Server 3.5 User's Guide

Copyright Notice

Copyright 2007 by HAURI Inc.

All rights reserved worldwide.

No part of this publication or software may be reproduced, transmitted, transcribed, stored in an archival system or translated into any languages, human or machine, in any form or by any means, electronic, mechanical, magnetic, chemical, manual, or otherwise, without the express written permission of Hauri, Inc.

Trademarks

ViRobot, HAURI are registered trademarks of HAURI Inc.

MS-DOS, MS Windows, MS Office, MS Outlook, and MS Outlook Express are registered trademarks of Microsoft Corporation, and other products or companies' names may be registered trademarks of their owners.

For ViRobot Windows Server 3.5 Users

This Manual is for Hauri customers who have purchased the ViRobot Windows Server 3.5 for your Server. It is strongly recommended that the user reads this manual before using the ViRobot Windows Server 3.5 to ensure effective use.

This ViRobot Windows Server 3.5 Manual may be slightly different from your program due to on-going functional improvements.

Table of Contents

Table of Figures

Chapter 1: About ViRobot Windows Server 3.5

Product Description

ViRobot Windows Server 3.5 is a strong vaccine product for server which is developed to protect the enterprise's server from virus, worm, malicious program and etc. As like Anti-virus, Network Security and Folder Protection, various security functions are integrated by one total product, and so management and operation is very convenient.

Key Features

Internal Source Access Policy Setting by Security Policy Wizard
A user can change easily the access policy for internal source including executable process, file, folder and network. Moreover, it intercepts computer virus or worm which is becoming high-technology and various by organic control of included functions.

Self-Protect of Security Program and Limitation of Configuration.
ViRobot Widows Server 3.5 supports Folder Protection function by itself to execute normally and correctly even if there is attack from virus or malicious code which interrupts the normal operation of security software as like computer virus vaccine, so the best performance and stability are supported to safely use PC all the time.

Support Security Center for security patch or shared resource
User can check the condition of OS security patch, shared folder and accounts and use Security Center function as like Internet Explorer Recover function, Virus information search, virus prevention tip and etc.

Quarantine function for files' isolation and backup
Because there are Quarantine to have custody of virus file and etc and Back-up draw to protect the backup file, if there is wrong detection, user can recover it.

Log & report of Server PC operation error
ViRobot Windows Server 3.5 records log about every kinds of attack, dangerous items and operation error. Moreover, it analyzes the data by various conditions and options and supports report, which is various kinds form, to user.

Chapter 2: ViRobot Windows Server 3.5 Installation

System Requirements

Platform: Windows 2003 Server / Windows 2000 Server / Windows NT 4.0 Server (SP 6 or above Recommended)
CPU: Pentium III 300 MHz or above Recommended
Memory: 256MB or above
Disk: More than 800 MB space Recommended
Others: IE 5.5 or above Recommended, TCP/IP support network Recommended
Supported Email Clients: MS Outlook, MS Outlook Express
Supported Instant Messenger: MSN

Installation

1. Run *ViRobot Windows Server 3.5* installation file.
2. Click the *Next* button to continue.
3. Read the *License Agreement* > Click *Yes* to continue.
4. Enter *User Name*, *Company Name*, and *License Key* information > Click *Next* to continue.

Note: You must fill in all the blanks to go to the next page. The word "None" can be used for the *Company Name* field.

1. Click the *Next* button to use the default installation directory.
2. Click the *Next* button to continue *ViRobot Windows Server 3.5* installation wizard
3. Wait while *ViRobot Windows Server 3.5* is installing.
4. Select both the *Update to the latest engine* and *Customer registration* options.
5. Click *Finish* and wait for updates to be installed automatically.
6. Fill out the Product Registration webpage.

Un-installation

1. Go to *Start* > *Programs* > *ViRobot Windows Server 3.5* > select *Uninstall ViRobot Windows Server 3.5* option
2. Click on the *OK* button in the *Confirm Uninstall* window.
3. Choose the *Yes* option to restart your computer.
4. Click on the *Finish* button.

Chapter 3: Anti-Virus

ViRobot Anti-virus offers reliable virus prevention, detection, and elimination program for your workstation. It automatically detects and repair infected files to keep your computer safe from viruses, worms, Trojan horses, and other threats.

How to enable/disable Real-time Monitor

1. Start *ViRobot Windows Server 3.5* program.
2. Left-click on the *Real-Time Monitor Configuration* link to the right of the program window as shown in Figure 1.
3. Check or uncheck the *Enable* option under the Anti Virus section to enable or disable ViRobot Real-time Monitor, respectively.
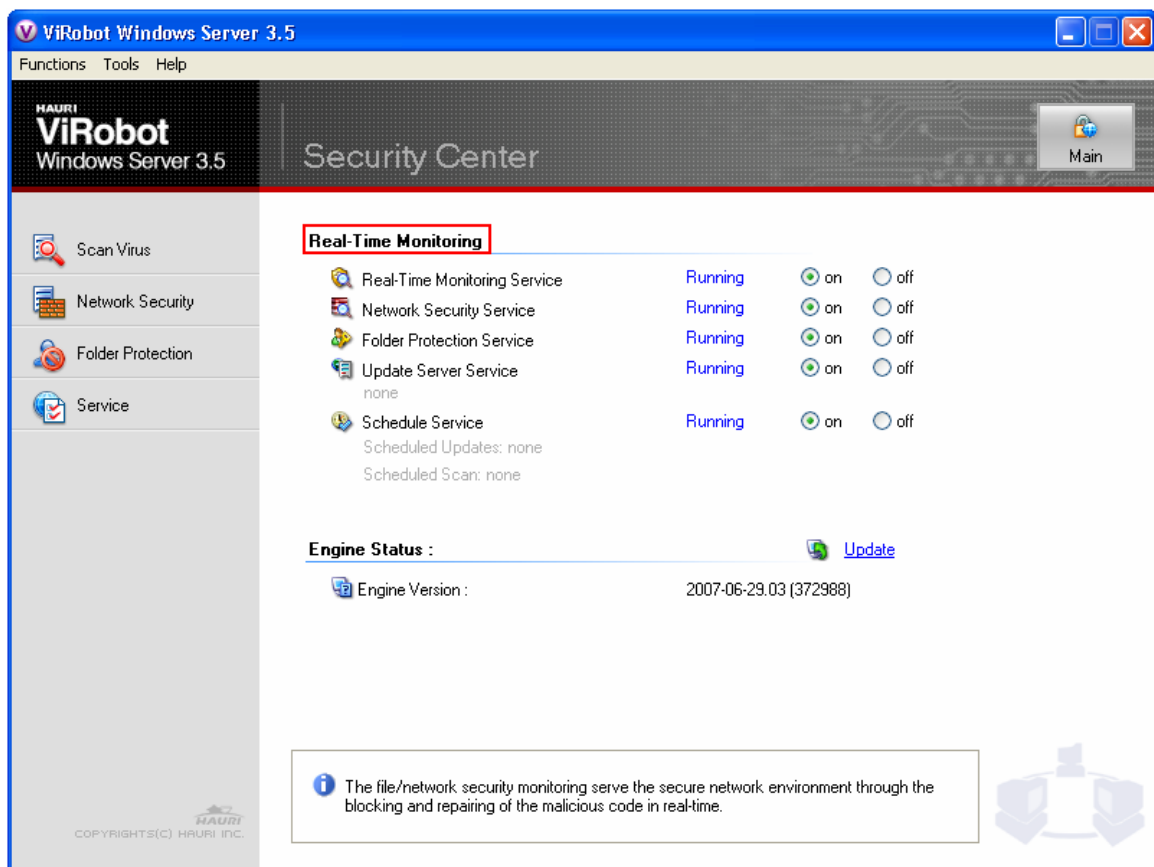
Figure 1: Real-Time Monitor Configurations

How to perform a quick scan

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Functions* menu > select the *Anti-Virus* option.
3. Select folders on the quick-scan list.
4. Click on the *Start Scan* button to start scanning selected quick-scan list (Figure 2).
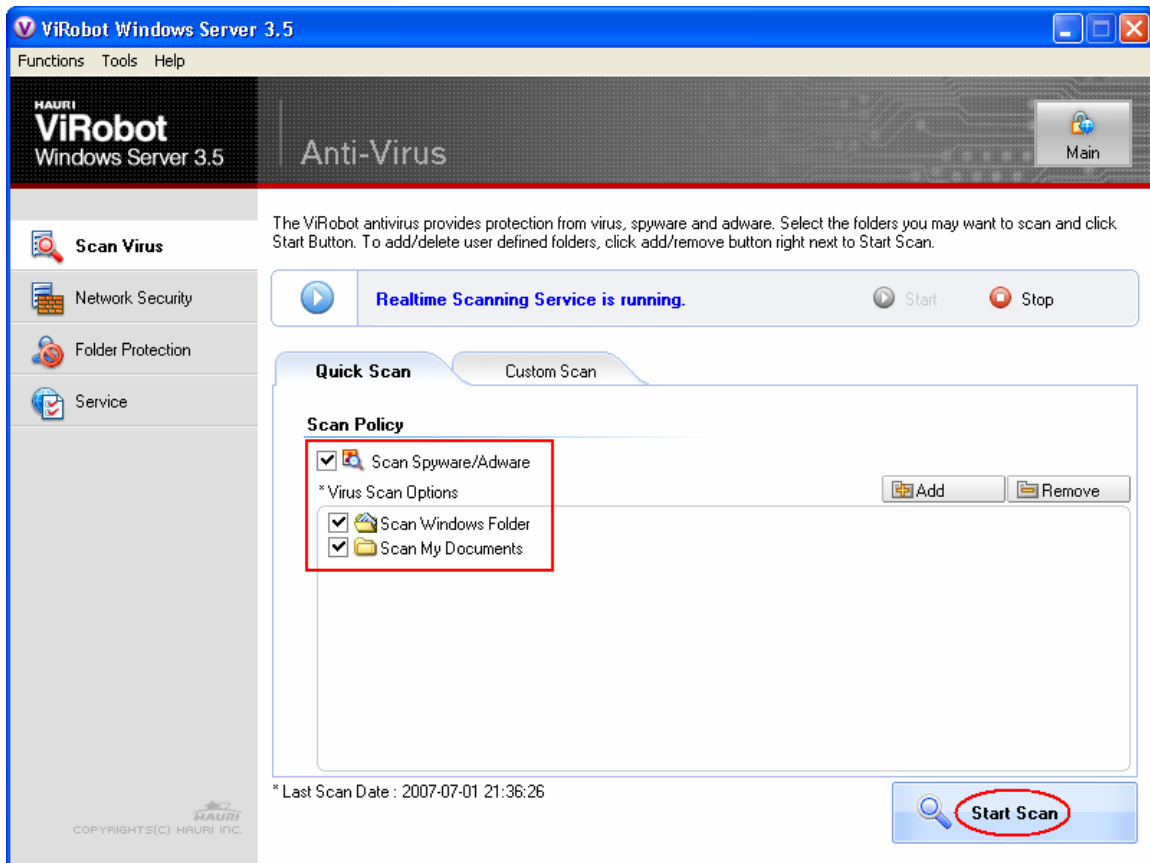
Figure 2: Quick Scan

How to modify your quick-scan list

To add a folder to your quick-scan list:

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Functions* menu> select the *Anti-Virus* option.
3. Left-click on the *Add (+)* icon at the bottom left corner of the *Quick Scan* tab.
4. Type in the name for a quick-scan folder you wish to create and customize, which will be displayed on your quick-scan list.
5. Choose the folder(s) you wish to include in the newly created quick-scan folder (Figure 3).

6. Click the *Apply* button.
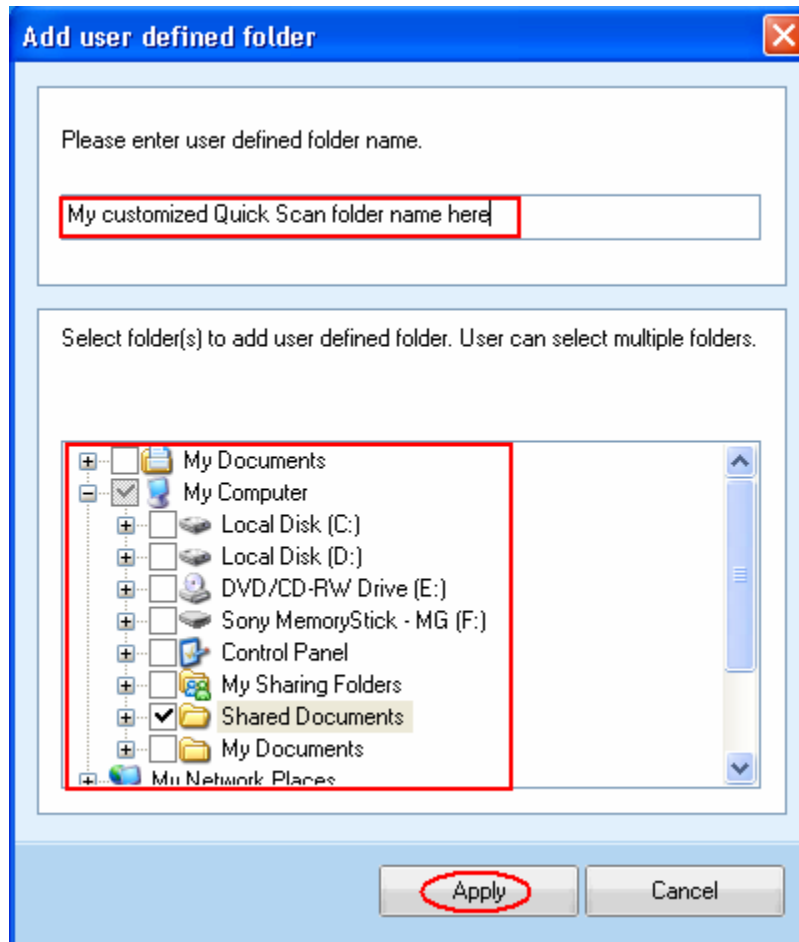
Figure 3: Add a Quick-Scan Folder

To remove a folder from your quick-scan list:

1. Left-click on the *Subtract (-)* icon at the bottom left corner of the *Quick Scan* tab.
2. Select a previously customized quick-scan folder to be removed.
3. Click the *Delete* button (Figure 4).
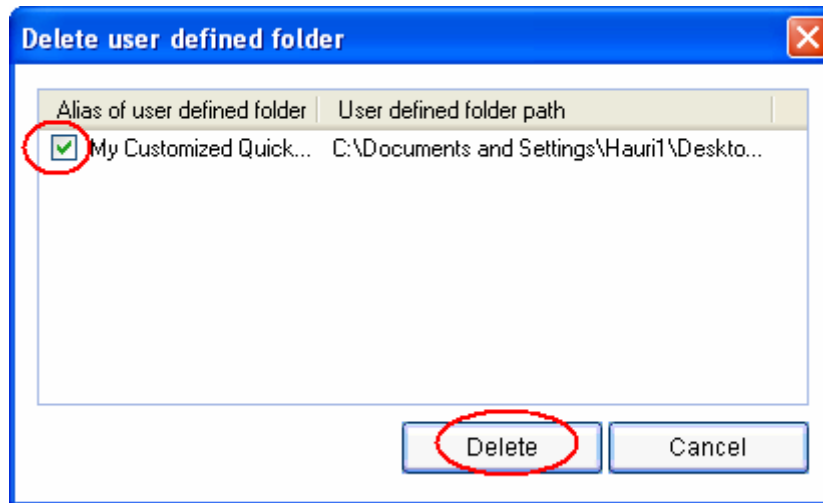
Figure 4: Remove a Quick-Scan Folder

How to perform a full scan of your system

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Functions* menu> select the *Anti-Virus* option.
3. Select the *Custom Scan* tab.
4. Select the drives and/or folders you wish to scan.
5. Click the *Start Scan* button.

How to configure basic Manual Scan settings

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Configurations* option.
3. Select the *Scan Virus* option under *Category* list on the left pane.
4. Under the *Manual Scan* tab, select basic manual scan configurations of your choice (Figure 5).
5. Click on the *Apply* button on the top Toolbar to save the changes.

Figure 5: Basic Manual Scan Settings

How to configure advanced options in Manual Scan

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Configurations* option.
3. Select the *Scan Virus* option under *Category* list on the left pane.
4. Under the *Manual Scan* tab, click the *Advanced Option* button

To configure compressed file settings:

1. Select the *Compressed files* tab.
2. Select a decompression level from the drop-down list (Figure 6).
3. Select other compressed file settings of your choice.
4. Click on the *Apply* button on the top Toolbar to save the changes.

Figure 6: Decompression Level Settings

To customize the User-defined File Extension list:

1. Select the *User defined file type* tab
2. To add a file extension to the user-defined list, type the file extension name, and click the *Add* button.
3. To remove a file extension from the user-defined list, hi-light the file extension name, and click the *Remove* button.
4. Click on the *Apply* button on the top Toolbar to save the changes.

To modify the Excluded Zone list:

1. Select the *Exclude Zone* tab.
2. To add a folder or a file to the excluded zone list, click the *Add* button, and choose a folder or a file of your choice.
3. To add a file extension, type in the file extension of your choice, and click the *Add* button.

4. To remove a folder, a file, or an extension, hi-light it, and click the **Remove** button.
5. Click on the *Apply* button on the top Toolbar to save the changes.

How to configure basic Real-time Monitor settings

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Configurations* option.
3. Select the *Scan Virus* option under *Category* on the left pane.
4. Choose the *Real-time Monitor* tab, and select basic real-time monitor configurations of your choice (Figure 7).
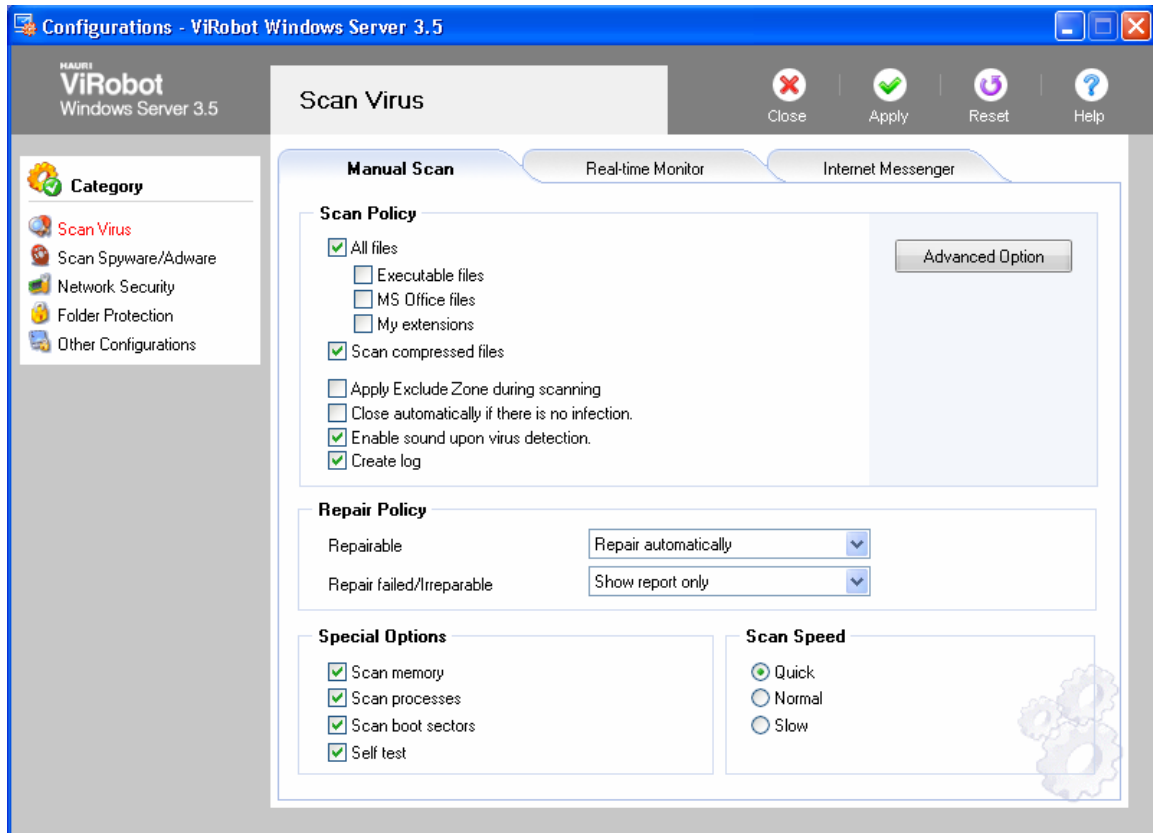5. Click on the *Apply* button on the top Toolbar to save the changes.

Figure 7: Basic Real-Time Monitor Settings

How to configure advanced options in Real-time Monitor

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Configurations* option.
3. Select the *Scan Virus* option under *Category* on the left pane.
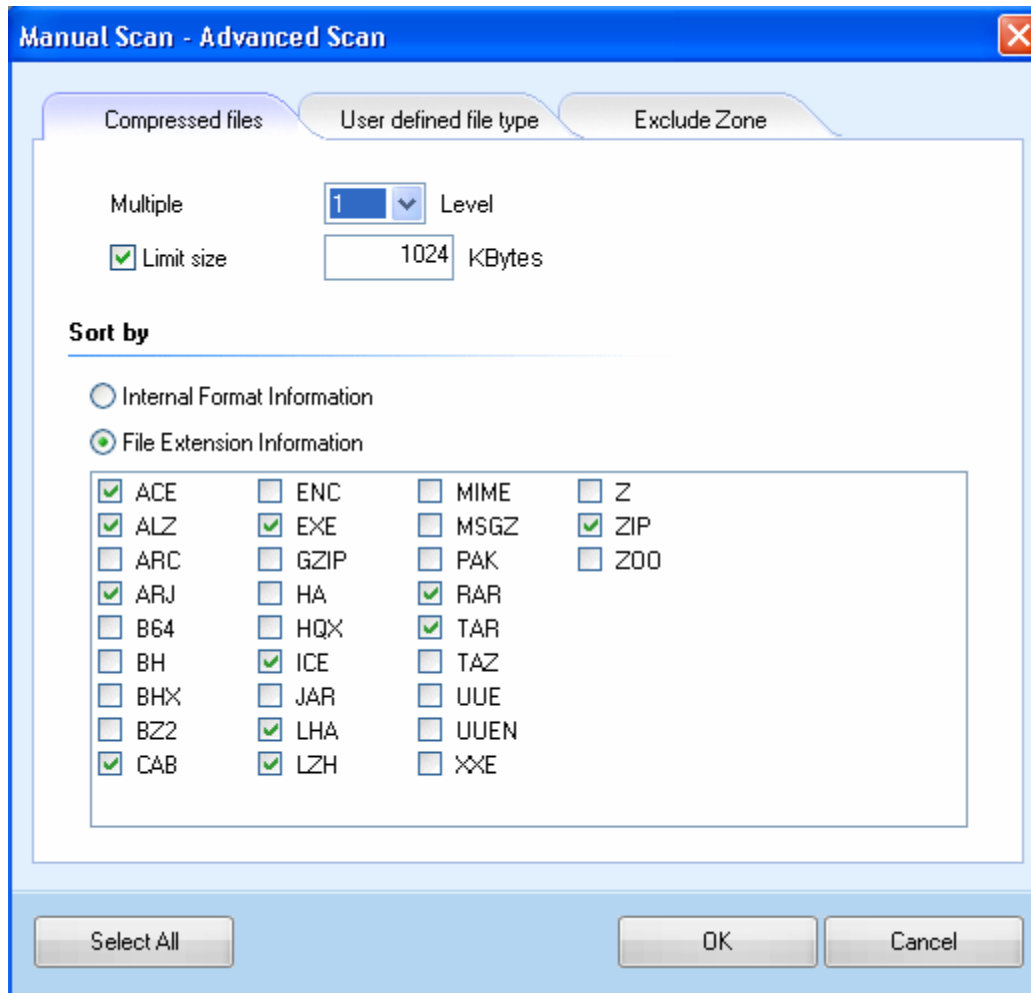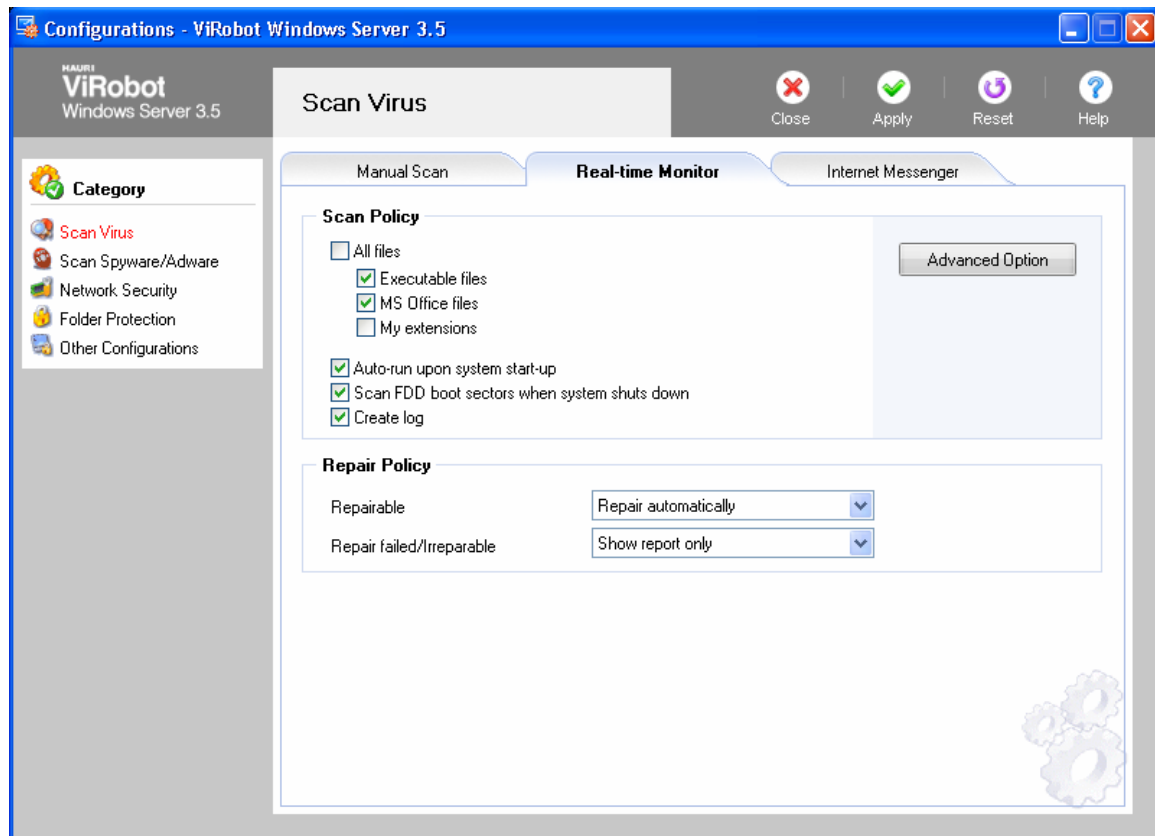
4. Under the **Real-time Monitor** tab, click the **Advanced Option** button.

To customize the User-defined File Extension list:

1. Select the **User defined file type** tab
2. To add a file extension to the user-defined list, type in the file extension name, and click the **Add** button.
3. To remove a file extension from the user-defined list, hi-light the file extension name, and click the **Remove** button.
4. Click on the **Apply** button on the top Toolbar to save the changes.

To modify the Excluded Zone list:

1. Select the **Exclude Zone** tab.
2. To add a folder, click the **Add** button, and choose a folder of your choice.
3. To remove a folder, hi-light it, and click the **Remove** button.
4. Click on the **Apply** button on the top Toolbar to save the changes.

How to restore/repair a file

1. Start **ViRobot Windows Server 3.5** program.
2. Go to the **Tools** menu> select the **Quarantines** option.

To restore/repair a quarantine file:

1. Select the **File Folder** option under **Quarantine** list on the left pane.
2. Choose your file(s).
3. Click **Repair** or **Restore** button to repair or restore the selected file(s), respectively.

To restore/repair a backup file:

1. Select the **File Folder** option under **Backup** list on the left pane.
2. Choose your file(s).
3. Click **Repair** or **Restore** button to repair or restore the selected file(s), respectively.

To submit a quarantine file:

1. Select the **File Folder** option under either **Quarantine** list on the left pane.
2. Choose your file(s).
3. Click the **Transmit** button to submit the selected file(s).

Chapter 4: Instant Messenger Monitor

ViRobot Windows Server 3.5 provides virus protection for instant messenger attachments. You can choose to scan files received by the instant messenger program. ViRobot Windows Server 3.5 automatically repairs or deletes the infected file once the virus is found.

How to set Instant Messenger Monitor configurations

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Configurations* option.
3. Select the *Scan Virus* option under *Category* on the left pane.
4. Choose the *Internet Messenger* tab, and select instant messenger configurations of your choice.
5. Click on the *Apply* button on the top Toolbar to save the changes.

Chapter 5: Update and Scan Schedule

Although you can manually check for updates at any time when you are connected to the Internet, ViRobot Windows Server 3.5 offers automatic checking for updates every specified time interval. The new ViRobot Windows Server 3.5 interface also provides you quick access to scheduled scan configurations.

How to enable and configure an Automatic Update schedule

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Update* option.
3. Click the *Configure* button in the lower-left corner of the *Hauri Update Service* window.
4. Select the *Enable automatic update* option.
5. Choose an update time interval, and other settings.
6. Click on the *OK* button to complete your selections.
7. Click the *Exit* button in the lower-right corner of the *Hauri Update Service* window.

How to add a Manual Scan schedule

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Schedule Wizard* option.
3. Click the *Add* button
4. Select a day and time from the drop-down arrows
5. Click the *Add* button, and select folder(s) or drive(s) to be scanned (Figure 8).
6. Click the *OK* button
7. *(Optional)* Check the *Hide virus scan window* checkbox to perform scheduled scans in background mode.
8. Click the *Done* button to see the newly created schedule on the schedule list.
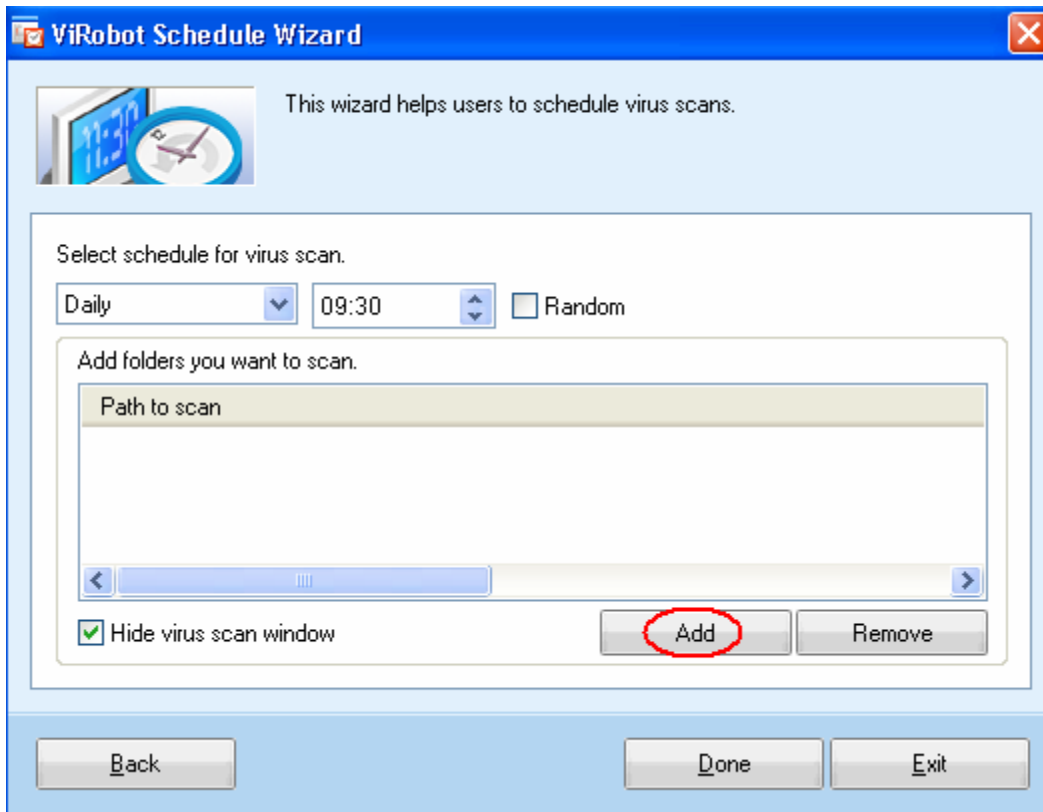9. Click the *Exit* button.

Figure 8: Add a Scan Schedule

How to perform a manual update

1. Start ***ViRobot Windows Server 3.5*** program.
2. Go to the ***Tools*** menu> select the ***Update*** option.
3. Click on the ***Update*** button.

Chapter 6: Anti-Spyware/Adware

You can configure ViRobot Windows Server 3.5 to scan for spyware/adware programs. By selecting this option, ViRobot identifies and removes spyware, adware, and other malware that intrude your privacy and slow down your system performance.

How to scan for spyware/adware

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Configurations* option.
3. Select the *Scan Spyware/Adware* option under *Category* on the left pane.
4. Check the *Scan Spyware/Adware* checkbox
5. *(Optional)* To monitor and repair spyware/adware automatically, check the *Enable* checkbox located in the *Spyware/Adware Monitoring* frame.
6. Click on the *Apply* button in the upper-left corner of the window.

How to set basic anti-spyware/adware configurations

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Configurations* option.
3. Select the *Scan Spyware/Adware* option under *Category* on the left pane (Figure 9).
4. Configure the anti-spyware/adware settings that suite you.
5. Click on the *Apply* button on the top Toolbar to save the changes.
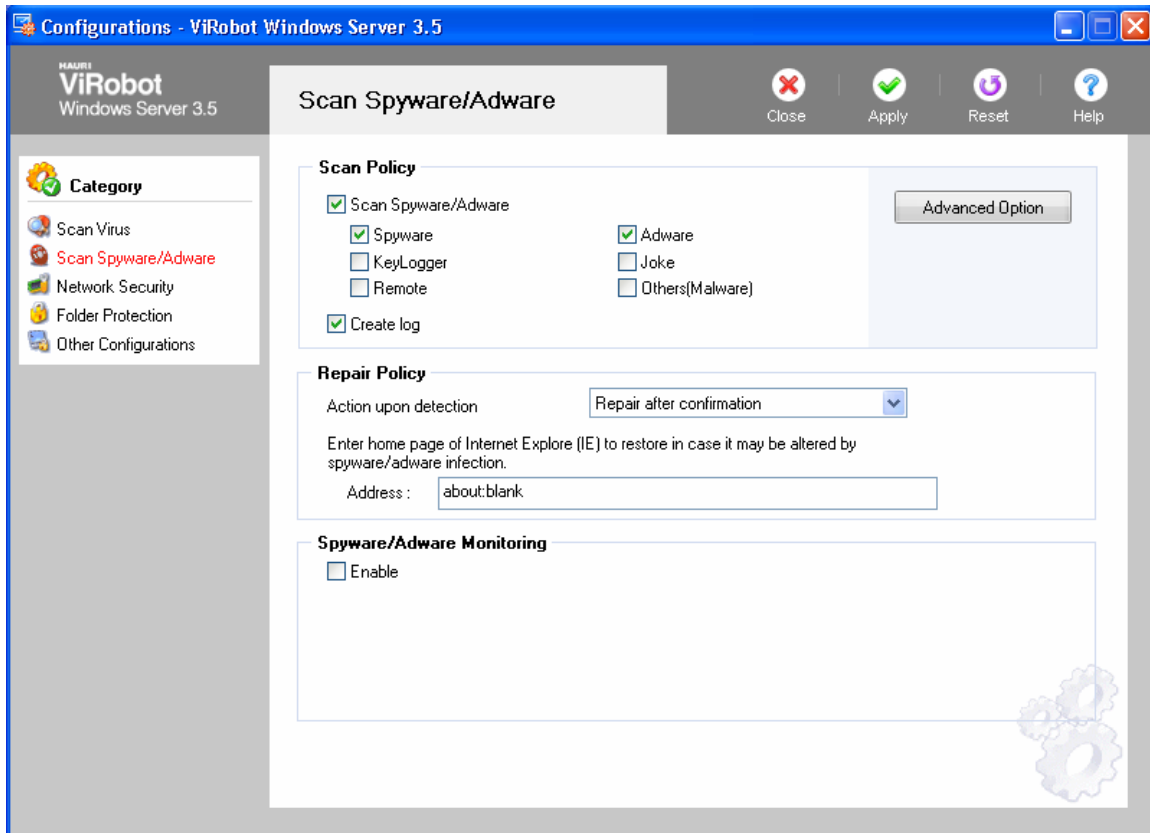
Figure 9: Anti-Spyware/Adware Configuration Window

How to configure advanced settings for anti-spyware/adware features

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Configurations* option.
3. Select the *Scan Spyware/Adware* option under *Category* on the left pane.
4. Click on the *Advanced Option* button located in the upper-right corner of the *Scan Spyware/Adware* page

To enable the advanced scan option:

1. Select the *Scan Policy* tab
2. Select the *Enable advanced scan* option.
3. Click the *Add* button, and choose a folder you wish to add to the advanced scan list.
4. Click the *OK* button.

Chapter 7: Network Security

ViRobot Network Security prevents unauthorized users from accessing your system to steal confidential data when you are on the Internet. It allows you to create your own firewall policy using Process Rule, Network Rule, and Shared Folder Rule.

How to enable/disable Network Security

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Functions* menu > select the Network Security option.
3. Click on the *Start* or *Stop* button to enable or disable Network Security, respectively.

How to prevent confidential data theft

To prevent confidential data theft:

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Functions* menu> select the Network Security option.
3. Click on the *Start* button to enable Network Security.
4. Select the *Enable outbound process rule* option.

To add a process to your Process Rule list:

1. Go to the *Rule* tab on the Network Security page.
2. Click on the *Settings* button.
3. Select the *Process Rule* option under *Select a rule* on the left pane.
4. Click on the *Add* button to browse for a process.
5. Click on the *Open* button to add the selected process.
6. Choose either *allow* or *deny* option for the selected process under the *Action* column (Figure 10).
7. Click on the *Apply* button to save the new process rule.
8. Click on the *OK* button to close the *Rule Manager* window.

Figure 10: Process Rule Configurations

To delete a process from your Process Rule list:

1. Go to the *Rule* tab on the Network Security page.
2. Click on the *Settings* button.
3. Select the *Process Rule* option under *Select a rule* on the left pane.
4. Hi-light a process you wish to delete from the Process Rule list
5. Click the *Delete* button.
6. Click on the *Apply* button to save the new change.
7. Click on the *OK* button to close the *Rule Manager* window.

How to block all network traffic

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Functions* menu> select the Network Security option.
3. Click on the *Start* button to enable Network Security.
4. Select the *Enable all network traffic blocking* option.

How to enable and customize Network rules

To enable your Network Rule option:

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Functions* menu> select the Network Security option.
3. Click on the *Start* button to enable Network Security.
4. Select the *Enable user defined network rule* option.

To add a network rule to your Network Rule list:

1. Go to the *Rule* tab on the Network Security page.
2. Click on the *Settings* button.
3. Select the *Network rule* option under *Select a rule* on the left pane.
4. Click on the *Add* button.
5. Type in the name for the network rule you wish to create and customize.
6. Set the configurations for your newly created rule including *Priority*, *Direction*, *Protocol*, *Action*, *IP Address*, *Port*, *Mode*, and *Description* (Figure 11).
7. Click on the *Apply* button to save the new network rule.
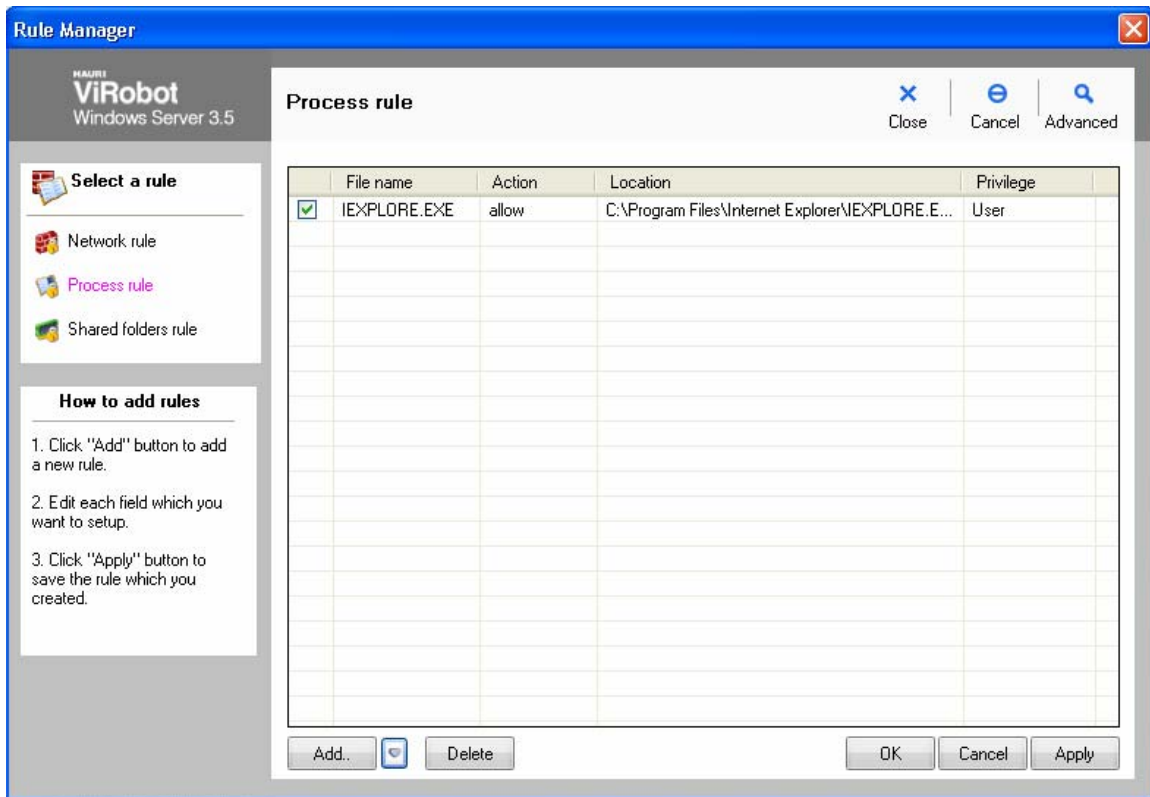8. Click on the *OK* button to close the *Rule Manager* window.

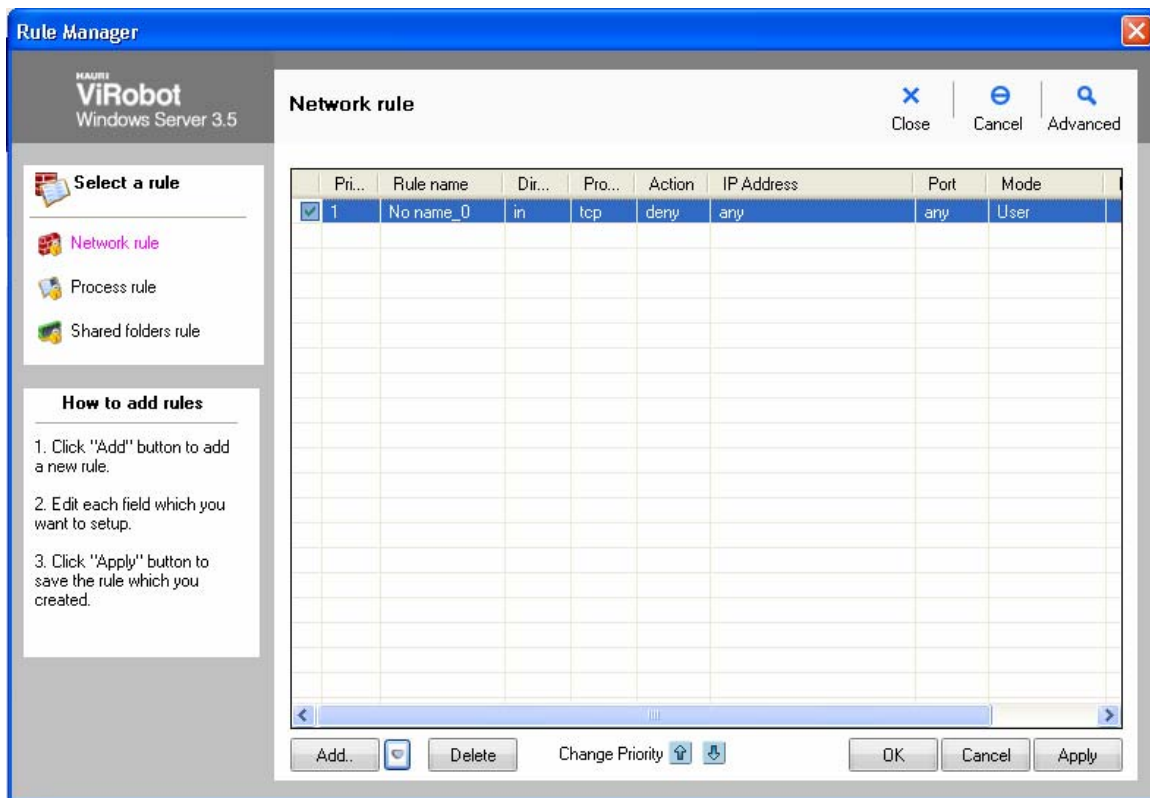**Figure 11: Network Rule Configurations**

To delete a process from your Process Rule list:

1. Go to the *Rule* tab on the Network Security page.
2. Click on the *Settings* button.
3. Select the *Network Rule* option under *Select a rule* on the left pane.
4. Hi-light a network rule you wish to delete from the Network Rule list
5. Click the *Delete* button.
6. Click on the *Apply* button to save the new change(s).
7. Click on the *OK* button to close the *Rule Manager* window.

How to customize Shared Folder rules

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Functions* menu> select the Network Security option.
3. Click on the *Start* button to enable Network Security.
4. Go to the *Rule* tab on the Network Security page.
5. Click on the *Settings* button.
6. Select the *Shared folders rule* option under *Select a rule* on the left pane.
7. Check the *Enable* checkbox.
8. Choose the configurations of your choice.
9. Click on the *Apply* button to save the new change(s).
10. Click on the *OK* button to close the *Rule Manager* window.

How to display the Network, Process, Shared Folder, and Network Status logs

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Functions* menu> select the Network Security option.
3. Select the *Log* tab.
4. Click on the *View Log* button.
5. Click on the *Network log*, *Process log*, *Shared folders log*, and *Network status* under *Select a log* on the left pane to view the log information of your choice.
6. Click the *Close* button to exit the *Log Viewer* window.

How to configure other Network Security settings

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Functions* menu> select the Network Security option.
3. Select the *Others* tab.
4. Select the Network Security configurations of your choice.

To select pre-defined Trojans to be blocked:

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Functions* menu> select Network Security option.
3. Click on the *Start* button to enable the Network Security (if applicable).
4. Go to the *Rule* tab on the Network Security page.
5. Click on the *Settings* button.
6. Click on the *Predefined Trojan* button (Figure 12).
7. Select the Trojan(s) you wish to block.
8. Click on the *OK* button to close the *Predefined Trojan viruses* window.
9. Close the *Rule Manager* window.

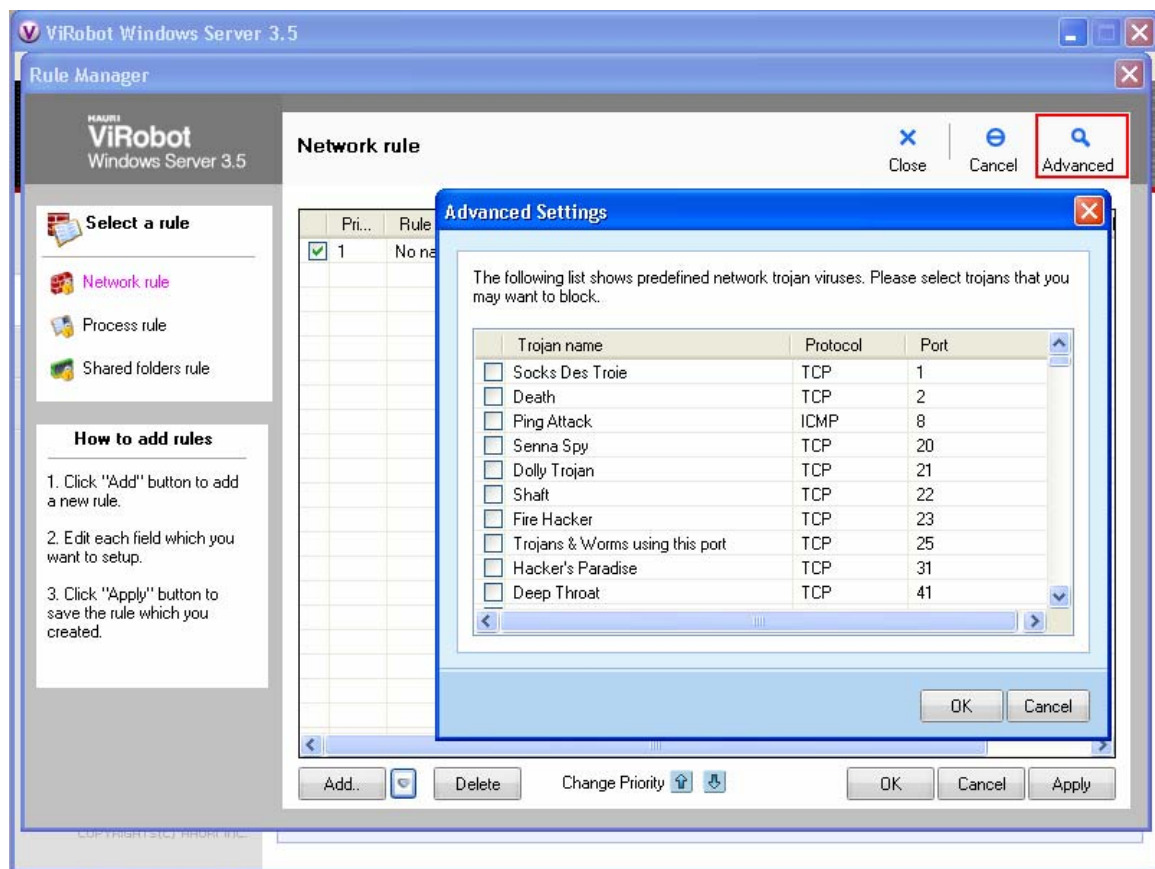**Figure 12: Pre-defined Trojan Settings**

Chapter 8: Security Vulnerability Identification

ViRobot Windows Server 3.5 analyzes Windows security vulnerabilities, shared folders, and user accounts. Additionally, this version of ViRobot Windows Server 3.5 provides easy access points to Windows security patches.

How to identify security vulnerabilities

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Functions* menu> select the *Service* option.
3. Click on the *Analyzing Security Vulnerabilities* link.

To scan for a list of MS Security Patches to be installed on your system:

1. Click on the *Security patches* tab
2. Wait for the program to generate a list of missing MS Security patches.
3. Once the missing patches are displayed, double click on an MS Security patch ID to view more information and/or install the missing patch from the Microsoft website.

To display a list of shared folder and user account information:

1. Click on the *Shared folders* tab to view all folders being shared on your system.
2. Click on the *Accounts* tab to view all user account information on your system. It also suggests security level of each account.

Chapter 9: Log Manager

The Log Manager displays detailed information into protection activities. ViRobot Windows Server 3.5 provides easy search options for users. You can configure how many activities you wish to record.

How to view different logs under Log Manager

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Log Manager* option.
3. Select an icon on the left Toolbar for a specific log type you wish to view or search.
4. Select *Search by*, *Date option*, *String option*, or *View log by* option from the corresponding drop-down menu.
5. Click on the *Search* button to view your search results.

How to delete a log entry

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Log Manager* option.
3. To remove a log entry, hi-light it, and go to the *Edit* menu > select the *Delete selected log* option. Multiple selections can be made.

How to export log information to a file

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Log Manager* option.
3. Select the log to be exported.
4. Go to the *File* menu > select the *Export to file* option
5. Choose a file format from the *File Format* drop-down menu.
6. Click on the *Save as a file* button.
7. Choose a location to save the exported log file
8. Click on the *OK* button on the *Complete* pop-up window.
9. Click on the *Close* button to exit the *Export to file* window.

Chapter 10: Other Features

This chapter describes how to configure other useful administrative tools and configurations.

How to configure Quarantine options

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Configurations* option.
3. Select the *Other Configurations* option under *Category* on the left pane.
4. Choose the quarantine configurations of your choice in the *Quarantine* frame.
5. Click on the *Apply* button on the top Toolbar to save the changes.

How to configure Log Manager options

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Configurations* option.
3. Select the *Other Configurations* option under *Category* on the left pane.
4. Choose the Log Manager configurations of your choice in the *Log Manager Option* frame.
5. Click on the *Apply* button on the top Toolbar to save the changes.

How to prevent ViRobot Windows Server 3.5 from being re-configured

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Configurations* option.
3. Select the *Other Configurations* option under *Category* on the left pane.

To set the ViRobot Windows Server 3.5 configuration password for the first time:

1. Type a password of your choice in the **New password** box. Your password should contain a combination of alphabets, numbers, and special characters (!, @, #, $...) of 8 entries or more.
2. Re-type your password in the *Confirm new password* box.
3. Click on the *OK* button.

To enable/disable the ViRobot Windows Server 3.5 configuration locking feature:

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Configurations* option.
3. Select the *Other Configurations* option under *Category* on the left pane.
4. Check or uncheck the *Enable Lockdown* option in the *Misc. Option* frame to enable or disable ViRobot Windows Server 3.5 configuration locking feature.
5. Click on the *Apply* button on the top Toolbar to save the changes.

How to enable/disable the R-Mouse scan option

1. Start *ViRobot Windows Server 3.5* program.
2. Go to the *Tools* menu> select the *Configurations* option.
3. Select the *Other Configurations* option under *Category* on the left pane.
4. Check or uncheck the *Enable R-Mouse Scan* option in the *Misc. Option* frame to enable or disable the R-Mouse scan option.
5. Click on the *Apply* button on the top Toolbar to save the changes.

Chapter 11: Contact Us

Customer Support Center

KOREA : HAURI Inc.
Homepage: http://www.hauri.net
Email: help@hauri.net
Tel: (82) 2-3676-1100
Fax: (82) 2-3676-8011